Published and Copyright (c) 1999 - 2013
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1511 03/15/13

~ Reuters' Keys Indicted ~ People Are Talking! ~ ESRB PSA Campaign!
~ U.S. To Press China! ~ "Ratters" Are Watching ~ Protecting Privacy!
~ No to SimCity Servers! ~ Nintendo Held Liable! ~ Facebook Hashtags!

-* Cyber Teams To Prevent Attacks *-
-* Wii U Could Be Nintendo’s First Flop *-
-* Cyber Attacks Leading Threat Against U.S.! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"

Happy St. Patrick’s Day!! We’re hoping that you’re all planning to help celebrate the wearin’ o’ the green this weekend. Plenty of green beer, some corned beef and cabbage, and a shamrock or two! Yes, we’re all a little Irish this weekend, so you may as well enjoy it.

Our latest snowstorm is all but a memory now. The accumulated snow is gone, with just a few small patches of snow sporadically littering the yard. Finally, we may be seeing some early signs of Spring. Now, if only the temperatures could stabilize a little higher than the past few days, I’d be happy!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Wii U Could Be Nintendo s First Flop!
SimCity Servers Not Necessary?
ESRB Will Launch PSA Campaign!
And much more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!

Wii U Could Be Nintendo s First Flop

Sales of Nintendo s (NTDOY) Wii U gaming console continue to falter, according to the latest retail figures. The NPD Group on Thursday released its U.S. video game sales figures for the month of February, which shows that overall sales of new hardware, software and accessories declined 25% year-over-year. Individual hardware sales were hit the hardest, dropping a whopping 36% from February 2012 as consumers wait for the Xbox 720"

and PlayStation 4.

All eyes were on Nintendo, however, following the company s disastrous January performance. Wii U sales were estimated to have only reached between 45,000 and 59,000 units during the first month of this year, marking one of the worst months for Nintendo in recent years.

Gamesultra reports that February sales were affected negatively by holiday returns when consumers couldn t resell the system at a profit as they could with the original Wii. But in its third month on shelves, sales of the Wii U improved slightly. NPD Group revealed that weekly sales on average increased around 40% in February, which Gamesultra estimates to mean that monthly sales of around 64,000 units.

Although sales increased, the Wii U continues to fall behind previous-generation consoles such as the Xbox 360 and PlayStation 3.

Maxis Insider Tells RPS: SimCity Servers Not Necessary

In all the fuss and mess of the disastrous SimCity launch, one refrain has been repeated again and again. While legions may be begging for an offline mode, EA representatives have been abundantly clear that this simply isn t possible. Maxis studio head, Lucy Bradshaw, has told both Polygon and Kotaku that they offload a significant amount of the calculations to our servers , and that it would take a significant amount of engineering work from our team to rewrite the game for single player.

A SimCity developer has got in touch with RPS to tell us that at least the first of these statements is not true. He claimed that the server is not handling calculations for non-social aspects of running the game, and that engineering a single-player mode would require minimal effort.

Our source, who we have verified worked directly on the project but obviously wishes to remain anonymous, has first-hand knowledge of how the game works. He has made it absolutely clear to us that this repeated claim of server-side calculations is at odds with the reality of the project he worked on. Our source explains:

> The servers are not handling any of the computation done to simulate the city you are playing. They are still acting as servers, doing some amount of computation to route messages of various types between both players and cities. As well, they re doing cloud storage of save games, interfacing with Origin, and all of that. But for the game itself? No, they re not doing anything. I have no idea why they re claiming otherwise. It s possible that Bradshaw misunderstood or was misinformed, but otherwise I m clueless.

People were already perplexed by EA s explanation of the impossibility of offline play. Kotaku ran a series of tests today, seeing how the game could run without an internet connection, finding it was happy for around 20 minutes before it realised it wasn t syncing to the servers. Something which would surely be impossible were the servers co-running the game itself. Markus Notch Persson just tweeted to his million followers that he managed to play offline too, despite EA s claims. And now with the information from our source, it would seem the claims just don t hold water.

So what are the servers doing? Well, alongside the obvious, of being involved in allowing players to share the same maps for their cities, and processing imports and exports between them, they re really there to check that players aren t cheating or hacking. However, these checks aren t in real-time in fact, they might take a few minutes, so couldn t be directly involved in your game.

Because of the way Glassbox was designed, simulation data had to go through a different pathway. The game would regularly pass updates to the server, and then the server would stick those messages in a huge queue along with the messages from everyone else playing. The server pulls messages off the queue, farms them out to other servers to be processed and then those servers send you a package of updates back. The amount of time it could take for you to get a server update responding to something you ve just done in the game could be as long as a few minutes. This is why they disabled Cheetah mode, by the way, to reduce by half the number of updates coming into the queue.

Clearly an offline game that included a single-player simulation of the region system derived from multiplayer would be more challenging to develop, but our source assured us that it was far from impossible.

So how difficult would it be for EA to create a single-player game that simply did away with the multiplayer-derived aspects and just let us build? It seems that lies somewhere between easy peasy and Bradshaw s claims of significant engineering . According to our source:

It wouldn t take very much engineering to give you a limited single-player game without all the nifty region stuff.

EA s claims about the necessity of online play claims that more people are seeing for themselves not to be true, just by running the game with the internet cable yanked out seem inexplicable.

We d obviously be very interested to hear a proper explanation.

ESRB Will Launch PSA Campaign To Educate Parents

A newly introduced national campaign will encourage parents to better monitor the games their children play by reviewing the Entertainment Software Rating Board s video game ratings.

The campaign, which will see the development of new Public Service Announcements in addition to the PSAs already in use by the ESRB, will also encourage parents to take advantage of the seldom-used parental controls on video game consoles.

The video game industry makes games for people of all ages, but that doesn t mean all games are appropriate for everyone, says U.S. Senator John Thune.

The more parents know about the wealth of dynamic tools the video game industry has developed for monitoring game play, the more empowered they will be to make informed decisions about which video games are appropriate for their family, adds Representative Debbie Wasserman Schultz.

Currently, 30% of parents do not regularly check the ESRB before making game purchases for their child. The new PSAs, which will be distributed to both local and national broadcast networks, will work to reduce this figure. Work will be undertaken to extend the current ESRB rating system to smartphone, tablet, and online social games, and game retailers will be using both their physical stores and their online networks to educate their customers.

Thune praises heightening the awareness of the ESRB ratings, saying, I commend the industry for raising awareness of the tools available to parents that can help them make informed decisions about the games their children play.

U.S. Jury Finds Nintendo Liable for Patent Infringement

A federal jury in New York on Wednesday found that video game company Nintendo Co infringed an inventor’s 3-D display technology patent with its handheld 3DS videogame system.

The jury awarded the inventor, Seijiro Tomita, $30.2 million in compensatory damages.

The patent relates to technology that Tomita developed for providing 3-D images without the need for 3-D glasses.

In opening arguments last month, Tomita’s attorney, Joe Diamante, told the jury in U.S. District Court in Manhattan that Nintendo used technology that Tomita developed for its 3DS. Tomita is a former longtime Sony Corp employee.

But Scott Lindvall, a defense attorney for the Super Mario Bros franchise creator, argued that the 3DS doesn’t use key aspects of Tomita’s patent.

Lindvall also said a 2003 meeting with Nintendo officials that Tomita cited in his argument was merely one of several the company held with vendors selling 3-D display technology.

Tomita, 58, sued Nintendo and its U.S. unit in 2011 for patent infringement. Tomita was not present in the courtroom on Wednesday.

"We are thankful to the jurors for their diligence and hard work," Diamante said in an e-mail after the verdict. "It has been a honor to represent Mr. Tomita and to protect his invention."

Lindvall declined to comment following the verdict. Nintendo officials were not immediately available for comment.

Violent Video Games Make People Violent. But So Do Pictures of Snakes.

The following blog was, unless otherwise noted, independently written by a member of Gamasutra’s game development community. The thoughts and opinions expressed here are not necessarily those of Gamasutra or its parent company.

Want to write your own blog post on Gamasutra? It’s easy! Click here to get started. Your post could be featured on Gamasutra’s home page, right alongside our award-winning articles and news stories.

Recently President Barack Obama called for more research into the link between violent video games and gun violence. More research isn t a bad thing, it isn t a bad thing at all. Since 1982 there have been 62 mass-shooting events in the United States alone. National tragedies, senseless acts of violence that each resulted in a tragic loss of life. News cycles target gun control, violence in films and music, and inevitably the discussion shifts to interactive media and video games.

For nearly thirty years we ve been having this discussion, asking the question: do violent movies, music or video games make people violent? Well according to Brad Bushman and Craig Anderson of Iowa State University, yes. Based on the results of their research they concluded in 2001 that video games and violent media can make people aggressive and violent. Based upon their data and their conclusions, however, it s safe to say that photos of snakes, crispy bacon, or a particularly rigorous game of chess can also make people aggressive and violent.

For all the vitriol on both sides of the debate, there s a shocking lack of attention given to the research and scholarship of the last three decades. It s a relatively small body of work, but despite its size some researchers particularly North American researchers have no problems with making broad, sweeping statements about their findings. Craig Anderson even likens the causal link between violent video games and violent behavior to the link between unprotected sex and HIV infection rates.

In 2004 the United Kingdom s Home Office conducted a meta-analysis of available and relevant scholarship regarding aggression and violent media, in particular video games. In the largest behavioral research database in the United States they found only thirty-five relevant articles that dealt with aggression and violence in video games, out of one hundred sixty-four thousand. Only twenty-two of those were from peer-reviewed journals and only nine of those sources dealt directly with violent video games.

It took forty years and thousands of studies before scientific communities within the U.S. could confidently claim that cigarettes were harmful, but based on a single study Anderson, Bushman and a handful of other scholars feel comfortable claiming an that there exists an undeniable link between a single factor in an individual s life and the development of aggressively violent behavior.

Unfortunately for Anderson and Bushman, the reality is much more nuanced.

The aggression they define in their study is a short-term increase in heart rate, blood pressure, and aggressive or competitive thoughts and actions. A reaction familiar to anyone who s ever played a competitive sport. It s also a familiar physiological response for anyone who s ever seen a photo of a snake or dangerous predator; it s a typical arousal response enhanced by competitive stimuli and excitement as indicated by any number of empirical studies on human autonomic responses. Music, films, TV, even books can elicit such a response from an average individual.

The BBC series Child of Our Time began in 2000 and set out to document the lives of several different newborns over a twenty-year span. In 2005, a

BBC film crew caught up with one of the children born at the beginning of the series. A young boy named Ethan, who was quite fond of violent video games, but who had an otherwise stable and supportive family life was observed before and after playing a round of the single player campaign in Halo.

Afterward, he was excitable, aggressive, argumentative, hyper-active and had difficulty settling down to go to bed. Clearly, the violence and excitement of an M-rated game had a negative effect on young Ethan. The next day at school, he was observed in the schoolyard.

What filmmakers saw was a well-adjusted boy who was very popular, likeable and played incredibly well with others. He exhibited above average prosocial behavior for his age and was described by his teachers as a bright and patient child.

Later, when Ethan played Halo against the inexperienced Professor Robert Wilson one of the show s creators he was reluctant to hurt his new friend. Instead he preferred to show Professor Wilson how to interact with the virtual world and how to play the game.

The discussion should not focus upon violent video games or violent visual media, it should focus on risk factors that might cause media to affect different people in different ways. Clearly, Ethan is not a representative case; he comes from an upper-middle class family, he is physically, socially and mentally healthy as a result of his surroundings and upbringing.

Anecdotal evidence is certainly not an adequate alternative for serious research and scholarship. But in this case, the time BBC filmmakers spent with Ethan and his family suggests that at the very least, the questions we need to be asking are not the questions we have been asking. There is no single cause of violence and likewise no single study that would provide conclusive proof that violence in visual media is harmful to all people, or healthy for all people.

Vladimir Nabokov s novel Lolita is the story about a middle-aged man pursuing a sexual relationship with an under-age girl. It s a story about modern romantic relations and the dangers of sexual temptation. But with such provocative subject matter, it becomes a very different story in the hands of a sexual predator than it is in the hands of a comparatively low-risk individual. Similarly, researchers like Jeanne Funk of the University of Toledo suggest that violent video games may provide a very different experience to children and adults with existing maladaptive disorders and other psychological risk factors. But because the bulk of the scientific research to come out of North America focuses upon experimental and lab-based research, and comes from a very narrow branch of academic psychology, there hasn t been a substantial effort by the academic community to re-frame the question in order to find answers that are more helpful than simply observing physiological responses.

Media does not create appetites or behaviors, but it can attract people with certain appetites or behaviors for whom the experience may be a very different thing.

If nothing else, the body of scholarship regarding violent video games and violent visual media suggests overwhelmingly that more research needs to be done. As it stands, most North American scholarship finds their causal and correlational links between violent media and real world violence in short-term experimental studies conducted in a lab setting.

While European scholarship finds little to indicate any connection between the two and instead places the emphasis on the social and longitudinal aspects of how violent video games fit into the lives of their subjects.

Guy Cumberbatch of the Video Standards Council, the leading media watchdog group in the UK, goes so far as to say:

> The evident weakness in the individual studies and the general pattern of inconsistent findings would not normally lead us to expect researchers to make any strong claims about video games. However, this is far from the case. As with other research on media violence, some of the strongest claims are made on the most flimsy of evidence.

Like any serious matter of public health, the discussion and investigation of the effects that violent visual media have on children and adults needs to be carried out with a measured tone, allowing the data to speak for itself. Unfortunately, too many studies to come out of North America reach conclusions that are at best incongruent with the data they present.

If the body of existing research is inadequate to fully answer the question at hand, perhaps then we might find at least some correlational information in crime statistics over the past fifteen years a period during which violent video games with exceptional levels of detail have come to dominate the holiday release cycles.

The world s three largest markets for video games are the United States, Japan and the United Kingdom. With that in mind, it stands to reason that the proportion of homicide or violent crime in the world s three largest markets for video games might show some similar trends. The populations of the US, Japan and UK are very different in both size and composition, but if violence in visual media in particular, video games had a tangible effect on the rates of violent crime we could expect to see similar levels of violent crime in all three nations.

Fortunately, this is not the case. Over the past ten years homicide rates in the US, Japan and UK have declined significantly. Additionally, in 2012 the United States had 4.8 homicides per hundred thousand people, while Japan and the UK had .4 and 1.2 respectively. The raw numbers are more shocking but the proportional estimates are a bit more illustrative: the three largest consumers of violent visual media have some of the lowest homicide rates in the world.

Assuming the existence of the causal link suggested by the work of Anderson, Bushman and others of their school of thought, it would be safe to assume that the homicide rates of the largest consumers of violent video games should be proportionally similar, and certainly not a illustrate decade long downward trend in all reports of violent crime.

Still, the knowledge base that we have is woefully inadequate. More research needs to be done, if not with the intention of finding a causal link between violence and violent media then certainly in order to identify which individuals might be more sensitive to violent media. However inadequate our current understanding of violent media in modern society may be, statistics and good, thoughtful, scholarship can point us in the right direction if we give them the attention they deserve.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Cyber Attacks Leading Threat Against U.S.

Intelligence leaders said for the first time on Tuesday that cyber attacks and cyber espionage have supplanted terrorism as the top security threat facing the United States.

That stark assessment, in an annual "worldwide threat" briefing that covered concerns as diverse as North Korea’s belligerence and Syria’s civil war, was reinforced in remarks by the spy chiefs before the Senate Intelligence Committee.

They expressed concern that computer technology is evolving so quickly it is hard for security experts to keep up.

"In some cases, the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks," James Clapper, the Director of National Intelligence, told the committee.

In written testimony, Clapper softened his analysis somewhat, playing down the likelihood of catastrophic attacks on the United States in the near term - either through digital technologies, or from foreign or domestic militants employing traditional violence.

But this year’s annual threat briefing underscored how, a decade after the Iraq war began and nearly two years after the killing of al Qaeda leader Osama bin Laden, digital assaults on government and computer networks have supplanted earlier security fears.

On Monday, White House national security adviser Tom Donilon, citing complaints from U.S. businesses about alleged Chinese cyber espionage, said the issue is a growing challenge to economic relations between the United States and China.

China said on Tuesday it was willing to meet Donilon’s request that Beijing talk with the United States about cyber security.

Last month, a private U.S. computer security company issued a study accusing a secretive Chinese military unit of being behind hacking attacks on a wide range of American industries.

China has denied such reports, and says it is a victim of cyber spying by the U.S. government.

The annual economic loss from cyber attacks is estimated to be in the tens of billions of dollars.

In a separate hearing on Tuesday before the Senate Armed Services committee, Army General Keith Alexander, head of the U.S. military’s Cyber Command, said cyber attacks on private companies and in particular on the U.S. banking sector were getting worse. He predicted that the intensity

and number of attacks will grow significantly throughout the year.

Alexander said the military was beefing up its cyber warrior team, adding troops from across the military as well as civilians. He said there would be three teams: a Cyber National Mission force which will deploy teams to defend against national-level threats; a Cyber Combat Mission force in charge of operational control; and a Cyber Protection force which will defend the military's information systems.

The goal is to add the new resources to the teams by the end of 2015, but one third of them are planned to be in place by this September.

Clapper also used Tuesday's Intelligence Committee hearing to give an alarming account of how U.S. intelligence capabilities will be damaged if Congress does not move to ease financial pressures caused by automatic across-the-board budget cuts known as sequestration.

Due to funding cutbacks, thousands of FBI employees could face furloughs, five thousand intelligence contractors could be terminated, cyber security efforts could be affected and older overhead intelligence collection systems - spy satellites - could face cutbacks, he said.

Intelligence agencies at a minimum want Congress to give them the authority to redistribute cuts among programs "to minimize the damage," he said.

Clapper presented to the Senate panel a 34-page paper that ran through a wide variety of threats covered by U.S. intelligence agencies, from continuing Middle East instability to what is predicted to be China's continuing domination of the world's supply of rare earth elements.

On two of the most volatile global crisis points, the U.S. spy agencies' assessment was restrained.

While Iran is improving its expertise in technologies including uranium enrichment and ballistic missiles, which could be used in a nuclear weapons program, the intelligence community does not believe Iran's leadership has decided to build a nuclear weapon and does not know if or when it might do so.

This assessment is consistent with a controversial 2007 finding, known as a National Intelligence Estimate, which concluded Tehran had "halted its nuclear weapons program" in fall 2003 and had not restarted it as of mid-2007, although it was keeping open the option of building nuclear weapons.

On Syria, U.S. spy agencies assessed that the erosion of the government of President Bashar al-Assad's ability to defend itself is accelerating.

Assad's forces have stopped insurgents from seizing cities such as Aleppo, Damascus and Homs, but the agencies say insurgents have been gaining strength in rural areas. This could ultimately lead to the establishment of a "more permanent base" for the rebels in Idlib province along the border with Turkey.

The listing of cyber-related attacks as the top item in the annual threat assessment is a departure from assessments offered previously. In 2011 and 2012, the first threat listed in the agencies' annual assessment to Congress was terrorism.

Pentagon Forming Cyber Teams To Prevent Attacks

The Defense Department is establishing a series of cyber teams charged with carrying out offensive operations to combat the threat of an electronic assault on the United States that could cause major damage and disruption to the country's vital infrastructure, a senior military official said Tuesday.

Gen. Keith Alexander, the top officer at U.S. Cyber Command, warned during testimony that the potential for an attack against the nation's electric grid and other essential systems is real and more aggressive steps need to be taken by the federal government and the private sector in order to improve digital defenses.

Alexander told the Senate Armed Services Committee that foreign leaders are deterred from launching cyberattacks on the United States because they know such a strike could be traced to its source and would generate a robust response.

But the country is not preventing what Alexander called "low-level harassment of private and public websites, property and information by other states." He did not mention any specific countries, even though the Obama administration is escalating its criticism of cyber thefts by China that have become intolerable to the international community.

Offensive cyber weapons are growing and evolving, Alexander said, and it is only a matter of time before tools developed by other nations wind up in the hands of extremist groups or even individuals who could do significant harm.

Alexander said 13 cyber teams are being formed for the mission of guarding the nation in cyberspace. He described them as "defend-the-nation" teams but stressed their role would be offensive. In comments to reporters after the hearing, Alexander likened the teams' duties to knocking an incoming missile out of the sky before it hits a target. He also said the teams would work outside the United States, but he did not say where.

He also said another 27 cyber teams are being established to support the military's warfighting commands while others will protect Defense Department's computer systems and data.

But even as Alexander detailed these moves, he pushed lawmakers to pass cybersecurity legislation that would make it easier for the government and the private sector which controls critical infrastructure such as the electric grid, banking systems, chemical facilities and water treatment systems to share detailed information about who is getting hacked and what to do about it.

President Barack Obama signed an executive order last month that relies heavily on participation from U.S. industry in creating new voluntary standards for protecting information and expands the government's effort to provide companies with threat data. But the order doesn't do enough to address the threat, administration officials said. Unresolved issues include the legal liability facing companies if they divulge information, and whether companies should be compelled to meet certain security standards.

The general also told the committee that there needs to be a clear consensus on how the nation is organized to protect critical infrastructure from cyberattacks. "It takes a team to operate in cyberspace," Alexander said. "But at times I think in talking about the team approach, we're not clear on who's in charge when."

Another issue that still needs to be settled is what constitutes an act of war in cyberspace, Alexander said. He does not consider cyberespionage and the theft of a corporation's intellectual property to be acts of war. But Alexander said, "I think you've crossed the line" if the intent is to disrupt or destroy U.S. infrastructure.

Sen. Carl Levin, D-Mich., the committee's chairman, noted that Obama recently issued a classified policy directive to govern cyber operations. The Pentagon also has developed a list of procedures on how to respond in "cyber crisis" situations, he added, and the Pentagon is expected to issue cyber rules of engagement for military commanders.

"The fact that these foundational policy frameworks and planning actions are just now taking shape serves as a stark illustration of how immature and complex this warfare domain remains," Levin said.

Alexander said the private sector maintains varying degrees of security over its computer systems. The financial industry typically is more secure than companies that operate the electric grid. Still, he said, banks are vulnerable to being disrupted by what are called denial of service attacks, a technique that works by overloading a website with traffic.

"The issue that we're weighing is, when does a nuisance become a real problem?" Alexander said. "And when are you prepared to step in for that? And that's the work that, I think, the administration is going through right now in highlighting that."

Alexander's testimony comes a day after Obama's national security adviser called for "serious steps" by China to stop cyber theft that has become intolerable to the international community.

The remarks on Monday by Tom Donilon before the Asia Society in New York underscore the growing concern in Washington over the security risks posed by cyber thefts and intrusions and the economic costs to U.S. businesses.

American companies are being more vocal about cyber theft emanating from China "on a very large scale." He said Beijing "should take serious steps to investigate and put a stop to these activities" and recognize the risk to international trade and to U.S.-China relations.

The Obama administration last month announced new efforts, including a new diplomatic push to discourage intellectual property theft abroad, to fight the growing theft of American trade secrets following the release of a report that linked China's military to the electronic theft of corporate trade secrets and U.S. government data.

After analyzing breaches that compromised more than 140 companies, the private security firm Mandiant has concluded that they can be linked to the People's Liberation Army's Unit 61398, a secret Chinese military organization based in Shanghai.

The Chinese government denied being involved in cyber theft, with China's defense minister calling the Mandiant report deeply flawed. China's Foreign Ministry said that country has also been a victim of hacking, much

of it traced to the United States.

Levin asked Alexander if U.S. intelligence agencies can determine not only which Chinese government organizations are stealing U.S. intellectual property, but also what Chinese companies may be receiving that intellectual property and using it to compete against U.S. firms.

But Alexander declined to be specific in open setting, saying only that the intelligence agencies have increased their capabilities in this area significantly over the last several years.

After the hearing, Alexander said he saw no reason to amplify Donilon’s remarks. "I agree with what Tom Donilon has put out there," he said. "I think it is absolutely on mark."

U.S. To Press China on Cyber Attacks, Seek Deeper Ties

Treasury Secretary Jack Lew will press China to take "serious steps" to stop cyber attacks directed at the United States and urge the administration of new Chinese President Xi Jinping to accelerate economic reforms, a U.S. official said on Friday.

Lew’s visit to Beijing on Tuesday and Wednesday comes at a crucial time, the official told reporters on condition of anonymity. "China is undergoing their once-in-a-decade leadership transition and, of course, their reform process is at a crossroads."

"It’s important to deepen our relationship with China’s new leadership team at this time," the official said.

Lew lacks the international stature of his predecessor, Timothy Geithner, and is signaling the importance the United States put on its economic relationship with China by making his first international trip as secretary to Beijing.

Secretary of State John Kerry in coming weeks will also make his first trip to China since taking office last month.

Both Kerry and Lew will host their Chinese counterparts in Washington in the middle of this year for the annual U.S-China Strategic and Economic Dialogue, the official said.

China’s legislature formally chose Li Keqiang as premier on Friday, installing the English-speaking bureaucrat as the man in charge of the world’s second-largest economy.

President Barack Obama raised U.S. concerns about computer hacking in a phone call with Xi on Thursday, just days after U.S. intelligence leaders said for the first time that cyber attacks and cyber espionage had supplanted terrorism as the top security threat facing the United States.

"We will press China to take serious steps to investigate and put a stop to these activities and to engage with us in a constructive direct dialogue to establish acceptable norms of behavior in cyberspace, recognizing it is a growing challenge for both of us," the senior U.S. official said.

Lew will also press China to allow its currency to rise further against the dollar and push on other concerns such as increased market access for U.S. goods and better protection of intellectual property rights, the official said.

China’s yuan has appreciated 16 percent in real terms against the dollar since June 2010. "More progress, however, is needed," the official said.

Thomson Reuters Employee Indicted for Aiding Hackers

A federal grand jury has indicted Matthew Keys, deputy social media editor at Reuters.com, for conspiring with members of the Anonymous hacking collective to break into the computers of his former employer, Tribune Co. The alleged incident occurred before he joined Thomson Reuters Corp, the indictment filed on Thursday indicated.

The indictment charged Keys with three criminal counts, including conspiracy to transmit information to damage a protected computer. The indictment said that he promised to give hackers access to Tribune Co. websites and that a story on the Tribune’s Los Angeles Times website was later altered by one of them.

Keys did not respond to requests for comment. But several hours after the indictment was handed down, he tweeted: "I found out the same way most of you did: From Twitter. Tonight I’m going to take a break. Tomorrow, business as usual." His attorney did not return a phone call seeking comment.

A Thomson Reuters spokesman said the company was aware of the indictment and added: "Any legal violations, or failures to comply with the company’s own strict set of principles and standards, can result in disciplinary action. We would also observe the indictment alleges the conduct occurred in December 2010; Mr. Keys joined Reuters in 2012."

The company did not comment on Keys’s employment status. However, a Thomson Reuters employee at the New York office where Keys worked said that his work station was being dismantled and that his security pass had been deactivated.

The documents in the case paint a picture of a disgruntled former Tribune employee who fell in with some of the most notorious hackers in the country and then worked with them, as well as against them.

The case began in early December 2010, when Fox 40, a Tribune-owned television station in Sacramento, Calif., received emails saying someone had claimed to have an internal list of employees, according to an affidavit for a search warrant submitted by Los Angeles-based Federal Bureau of Investigation agent Gabriel Andrews.

A former colleague suggested Keys as a suspect, according to the FBI affidavit, because he had been terminated as an employee in October 2010 and then refused to hand over control of the Facebook and Twitter accounts he had run for Fox 40.

Within weeks of the first suspicious email, the affidavit said Keys told the same colleague that he had penetrated an elite chat group used by some of the most sophisticated members of Anonymous. According to the

affidavit, Keys said he had learned of upcoming attacks on the Tribune's Los Angeles Times, eBay's PayPal and other companies. Two days later, a story on Latimes.com was defaced.

When Keys learned that a member of the hacking group had changed the Times story, Keys responded "nice," according to the indictment.

Transcripts of the electronic chats excerpted in the affidavit and the indictment show someone using the nickname AESCracked offered to grant access to Tribune computers to others in the chat group. "Let me see if I can find some other users/pass I created while there," he wrote after previous credentials were denied access, the indictment said. The indictment says Keys used the nickname AESCracked.

The documents appear to show Keys playing a double game for weeks before getting kicked out of the chat group. As a journalist between jobs, he took screenshots of the hacking group's chats and sent them to media outlets, he wrote later on a personal blog cited by the FBI.

He claimed credit for that work in a posting on his personal website in March 2011, writing: "I identified myself as a journalist during my interaction."

But others in the chat room were furious at the leaks. The leading figure, known as Sabu, said on Twitter days later that Keys was AESCracked and "gave full control of LATimes.com to hackers."

Sabu, subsequently identified as Hector Xavier Monsegur, was arrested later in 2011 and began cooperating secretly with the FBI while continuing to lead an Anonymous spinoff called LulzSec, according to court documents.

The probe of Monsegur, who is awaiting sentencing for more serious breaches at Sony and elsewhere and is continuing to cooperate with prosecutors, led to chat transcripts containing evidence against Keys, the affidavit says.

Keys, now 26 and living in New Jersey, went to work for another television station before joining Reuters in January 2012 as deputy social media editor. He was relatively well known on Twitter, amassing more than 23,000 followers for his personal account, apart from his tweets under the Reuters brand.

He also wrote occasional longer blog entries for Reuters, including at least two about Anonymous. In a March 2012 entry, after Sabu's exposure, Keys blogged about how he had gained entry to the elite chat group called InternetFeds and said Sabu had confided his New York location and other details.

One Sacramento acquaintance, Mona Vaughn, said Keys had "a pretty extreme personality." She said she recommended him on LinkedIn before she found out that he had disparaged a former employer.

At Reuters, where his main mission was to promote journalists' stories through social media, Keys drew attention last October by covertly creating a parody Twitter account, PendingLarry, which mocked Google after a premature release of an earnings report that included a space reserved for comment by CEO Larry Page. He was reprimanded by Reuters editors for that incident.

The case against Keys is being prosecuted by Benjamin Wagner, U.S. Attorney for the Eastern District of California, which includes Sacramento. Keys could face a maximum of 25 years in prison.

In an interview, Wagner said that Keys appeared to have been acting against Tribune primarily as an angry former employee.

But because Keys could have claimed he was acting as a journalist, Wagner said the case was taken to high-level officials at the Justice Department in Washington for approval multiple times "out of an abundance of caution." Wagner declined to say whether Keys has been cooperating.

Some online activists used the Keys case to renew their criticism of the Computer Fraud and Abuse Act (CFAA), the anti-hacking law under which Keys was indicted. Federal prosecutors used the law against Aaron Swartz, a computer programmer who was accused of illegally distributing scholarly articles and hanged himself in January.

Hanni Fakhoury, an attorney at the Electronic Frontier Foundation, said the cases were fundamentally different but both highlighted the excessively draconian punishments that prosecutors could seek under the CFAA.

"Aaron’s case was about taking information in a way he wasn’t supposed to, and this is about vandalism in its simplest form," Fakhoury said. "But the similarities are in how the sentencing scheme is so dramatic under the CFAA that he (Keys) could face 25 years."

Keys is scheduled to be arraigned on April 12 in Sacramento, according to the court docket.

The case in U.S. District Court, Eastern District of California, is United States of America v. Matthew Keys, 13-82.

Proposal Protects Workers’ Social Media Privacy

Employers would be prohibited from requesting the username and password of an applicant or employee’s social media account under a measure presented Thursday to the House Business and Labor Committee.

Bill sponsor Sen. Anders Blewett, D-Great Falls, said the proposal would fill a void in Montana law to prevent employers from requesting the "keys to someone’s personal life" on social media websites such as Facebook and personal email accounts.

In 2009, the city of Bozeman requested that potential employees relinquish their social media and personal email usernames and passwords before accepting employment with the city. The city abruptly ended the practice after public outcry.

"I would analogize a private Facebook account, a private Gmail account, no different than a house with a lock on it," Blewett said.

The measure, Senate Bill 195, wouldn’t bar an employer from creating restrictions that prohibit employees from using Facebook or other distracting sites during the workday.

The bill also was amended to allow disclosure of usernames and passwords for business Internet accounts and ensures employers the right to complete thorough background checks of potential employees.

Opponents argued the measure would curb employers' ability to monitor their employees' behavior, particularly if the employee posts sensitive client information on a social media site. Employers also need the information to conduct internal inquiries into employee harassment and fraud, they said.

"This bill would prohibit an employer from actually conducting an investigation into a situation where they suspect that one of their employees is conducting corporate espionage," said Mark Baker, a lobbyist representing the Kalispell Chamber of Commerce.

Blewett dismissed the arguments, saying such employers want to do the jobs of law enforcement officers in cases of criminal activity, and employers retain the right to establish rules pertaining to Internet use in the workplace.

"The question is how far does an employer have to go when they are screening potential employees," Blewett said. "This law would make it clear that they don't have to go and ask for the keys of someone's personal life."

The measure passed the Senate with a 48-2 vote and needs the committee's endorsement to move to the full House.

Ratters They Watch Through Your Webcam

From hundreds of miles away, a man sits at his monitor watching an unsuspecting woman use her computer, undress and go to sleep. She has no idea she s being watched. The remote attacker has installed software to control her webcam. What s worse, he s recording all of her actions and posting those videos on YouTube or trading the videos with other voyeurs online.

This scenario is happening more and more; there are myriad photos and videos available online indicating the practice is getting easier and more popular with an online community called Ratters. They use Remote Access Tools (R.A.T.s) to activate the webcams of compromised computers and record video of unsuspecting users. They call the owners of these infected computers slaves, and compromising videos, especially of female slaves, are openly traded, and posted on YouTube.

The practice of taking over a computer is not new. Hackers have produced software for years that gives complete control of a machine to a remote attacker. Aspects of these tools are also common in the IT field for offering remote tech support. But what s new is the community of remote attackers who have formed in hacking forums to share or trade access to the enslaved computers and talk about their exploits.

In a detailed article on Ars Technica, journalist Nate Anderson probes into the members at hackforums.net, which he says has more than 134 pages of posts featuring captured images and video of female slaves. Some are recorded from webcams, and others are videos or images found on the hard drives of compromised computers that their owners thought were private

and secure.

Beyond invading a victim s privacy, Ratters have tools in their software to scare or annoy remote victims. They can open and close their DVD drives, display graphic images on screen, have the computer read aloud using text-to-speech applications, or even hide the start button.

While this type of unauthorized computer intrusion is clearly against the law, the fight against Ratting is a challenge. There are many free or low-cost programs already available online, attackers are not usually local or in close proximity to victims, and while any one forum of Ratters could be shut down, others could easily pop up elsewhere.

Victims are infected with remote access tools the same way many viruses spread: opening attachments, drive-by downloads from sketchy sites, downloading files from torrents or file-sharing sites, or being tricked into clicking links through social media sites.

The good news is that these tools can be detected and held at bay. First, pay attention to the little light next to your webcam. If at anytime it s lit and you aren t using your webcam, find out why it s engaged by running either an antivirus program or hitting ctrl-alt-del to see what processes are actively running. If you see anything suspicious, it s time to disconnect from the Internet and disinfect.

Best practices to stay safe include using a firewall, keeping all software up to date, and using an anti-virus program. Also, staying away from torrent sites and sketchy websites will add a layer of protection, as many Ratters seed files on these sites disguised as free videos, music or software programs. If your paranoia is high and you really want to be sure your webcam isn t spying on you, some have suggested taping a piece of paper over the camera, but this does nothing to protect your information or image/video files already on your computer.

Facebook Plans To Introduce Hashtags

Facebook might become a bit more like Twitter soon. According to reports from The Wall Street Journal and All Things D, Facebook is experimenting with using a popular Twitter feature - the hashtag.

According to the reports, Facebook is working on ways to incorporate the hashtag into the service. Like it does on Twitter, the #+word combination would group conversations around specific topics. Currently on Facebook you can tag a topic or person who has a Facebook account or page, but you cannot simply see what all Facebook users are saying about a specific topic.

But it might be a while before you start seeing the # symbol showing up in your feed. "It is unclear how far along Facebook’s work on the hashtag is and the feature isn’t likely to be introduced imminently," the Wall Street Journal reported yesterday. When reached by ABC News, a Facebook spokesperson said, "We do not comment on rumor or speculation."

Instagram, which was purchased by Facebook for $1 billion last year, also incorporates the hashtag. Users can tag their photos with hashtags and they will be grouped together when you select that tag. The functionality would also keep people on Facebook longer and talking about

specific topics, all which would be a boon for Facebook's advertisers, the Journal said.

The functionality would also complement Facebook's new News Feed, which was introduced last week. The new feed allows users to see feeds with just specific types of content, including photos, games and music. This week Facebook also rolled out a new design to its Timeline, which groups status and updates on the left side and content and apps on the right.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.